veea™

The New Edge: The Home Office

Simple and Secure Remote Work Environment for the New Normal

The New Edge: The Home Office

Simple and Secure Remote Work Environment for the New Normal

Table of Contents

The Zero Commute Lifestyle: Work-From-Home (WFH)

Your employee's office today is wherever they conduct business most effectively—and due to the COVID-19 pandemic, that is likely no longer in your corporate headquarters or a branch office.

In 2020, companies responded quickly to the pandemic with temporary solutions for remote worker connectivity and computing. Many leveraged personal devices and shared home Wi-Fi solutions with family members where they competed for bandwidth and reliable connectivity. In addition, companies sacrificed enterprise-grade data security for the need to keep business moving. These temporary solutions led to a mingling of personal and company data on remote machines, and hackers noticed.

Today, as many employers consider the post-COVID-19 workplace, they are no longer viewing remote work as a perk. Many high-value employees are unwilling to give up their new-found freedom and cost savings, and many companies have found that worker productivity increased when they worked at home. As a result, many companies are migrating to a hybrid or even permanent home-based workforce model. Many refer to this as the `new normal', and it will create additional challenges for IT professionals.

For nearly twenty years, IT planners prepared for approximately 20% of their workforce to use remote technology, with the other 80% resident in centralized physical offices. During the pandemic, those numbers reversed.

Moving Beyond Stopgaps Quickly

Moving forward, companies need to do more to protect and empower their workforce and their business. Remote work, whether full-time or a few days a week, is here to stay. Normal has been forever redefined, and security programs will need to adapt accordingly.

Businesses need a permanent remote access solution for home-based workers that is secure yet simple and cost-sensitive. The solution must be simple for users, simple to configure, and simple to manage. Minimizing IT resource requirements while also having the ability to scale as needed has driven many companies to a SaaS model for their applications and services. Secure remote access is a good managed service candidate.

Connectivity with robust security is more important than ever before. With the significant increase in home-based remote work, the use of laptops and mobile devices connecting to your network from outside your firewall has increased significantly. And that change is here to stay. You need a comprehensive security service that will safeguard the data and workflows associated with the devices connecting to your network—a front line of defense against security threats.

IT Challenges Supporting Home-Based Workers

Companies must enable a remote work environment that eliminates any IT-related barriers that might adversely affect employee productivity. Typical options for the home office lack the same robust experience available in a branch office or at headquarters—fast connectivity, processing power, and secure access.

1 **A plug-and-play solution –** Workers need a device that is simple to plug in and autoconfigures in minutes. IT can benefit from a fully-managed service that can be deployed with a minimal OPEX and CAPEX commitment for a lower Total Cost of Ownership (TCO) than corporations can provide on their own.

2 **Wi-Fi, Ethernet, and wireless broadband connectivity –** Remote users need flexible connectivity. Wi-Fi is subject to more interference than a wired connection and can be affected by the layout of a home, objects blocking the signal, interference from electrical devices, or neighbors' Wi-Fi networks. Having a wired back-up option is critical to providing a productive remote work environment. Ethernet connectivity can overcome poor Wi-Fi signals, and dedicated 4G connectivity can address bandwidth issues.

3 **Improved worker productivity –** Dedicated mobile network connectivity improves performance and reliability, and eliminates the need to share a broadband connection with family members.

4 **Connectivity protection for all devices –** Employees work with a wide variety of devices and platforms. IT needs to ensure that all devices are protected against Malware, DDoS, and Ransomware attacks via a single endpoint enforcement that does not require installation and continuous updating of security clients on each individual device.

5 **Protect data-in-motion –** More employees working from home, more endpoints, and more data-in-motion outside the corporate firewall increase the risk that data will fall into the wrong hands. IT needs a work-from-home solution with a full security stack for end-to-end security.

6 **Central management and control –** Most IT teams were not designed to handle a large remote workforce, and the influx of support calls during Covid-19 put a severe strain on help desks. Old tools cannot manage WFH solutions. More visibility and control at the edge is required to effectively support remote user issues.

7 **Ability to scale and add additional capabilities for remote workers in the future –** As remote work technology evolves, IT needs the ability to deploy new services and capabilities easily to WFH environments.

8 **A cost-sensitive solution –** Support and help desk costs have risen dramatically with remote work because there are so many variables beyond company control. A feature-rich, cost-sensitive solution is needed to scale and support a large number of WFH workers.

Why VPNs Are Not Enough to Secure Data-in-Motion

Today, data is contantly in motion – data in transit across networks. For years, businesses have assumed that VPNs create a secure, private tunnel that allows communications and data to traverse safely over public, non-secure networks. But cybercriminals have become sophisticated, and have exposed four VPN security vulnerabilities, resulting in several high-visibility data breaches and attacks.

1 **VPNs often have outdated encryption protocols because businesses aren't vigilant and consistent about updating their VPN software.**

2 **VPNs don't inspect and filter both incoming and outgoing traffic, which allows some security threats to slip through.**

3 **VPNs typically require manual, high-touch administration, which introduces human error into the security equation.**

4 **VPNs can be prone to social engineering attacks. If a hacker steals your login credentials, they can access your network.**

Hackers exploit these vulnerabilities using man-in-the-middle (MITM) attacks to intercept sensitive data-in-motion from the remote user's device to the company's workplace. Companies need to stop MITM attacks and a host of other cyber threats such as DDoS attacks, phishing, and data theft to secure data-in-motion from any device to any environment (cloud, data center, etc.).

The vTPN Security Service

The vTPN Security Service delivers a full-stack security solution that uniquely meets your organization's and distributed workforces' needs. Vulnerable data-in-motion is protected between user endpoints, including those in remote worker home offices, and the enterprise and cloud data services that support them. The vTPN Security Service offers a full spectrum of protection against cyberattacks, unauthorized access and intrusion, malware, DOS/DDOS attacks, malicious service interruption, ransomware, and botnets.

Everything Your Remote Employees Need

All the capabilities, services, and controls you need to secure your employees WFH IT environment.

Every Way Your Remote Employees Work

Support for all IT environments, including public/private clouds, remote offices, and all popular mobile devices, with the power to support SaaS enterprise applications.

Unauthorized Remote Access

- Man-in-the-middle attacks
- Unauthorized surveillance
- Encryption compromises
- Device compromises
- Advanced persistent threats
- Network breaches due to human factors
- Adjacent network vulnerabilities
- Latent pre-existing breaches

DDoS and Malicious Service Interruption

- DoS and DDoS attacks
- Site defacement and site control
- Bot / Zombie attacks

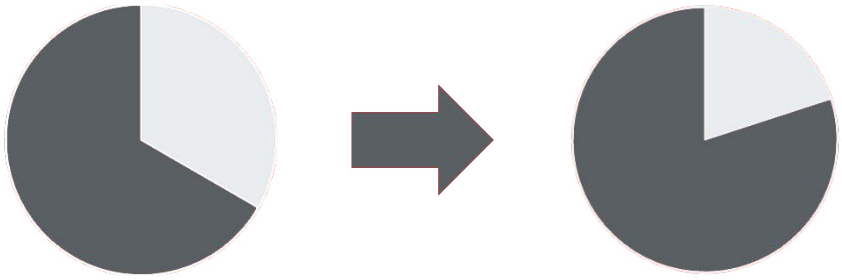
Outbound Control and Data Loss Prevention

- Unauthorized site visitation
- Unauthorized user access
- Unauthorized device registrations
- Rogue employees
- Botnet / Zombie attacks
- Data and information loss

Inbound Controls and Content Screening

- Virus and Worm infections
- Malware
- Ransomware
- Trojan and Spyware

VPNs Don’t Deliver the Full-Stack Security Protection Your Workers Need



2/3 of enterprises experience serious security breach attempts and data loss/compromise

Ponemon Institute, IBM

80+% of security breaches involved **data-in-motion** incidents

IDC

56% of employees have used their own personal computers as their work device during COVID19.

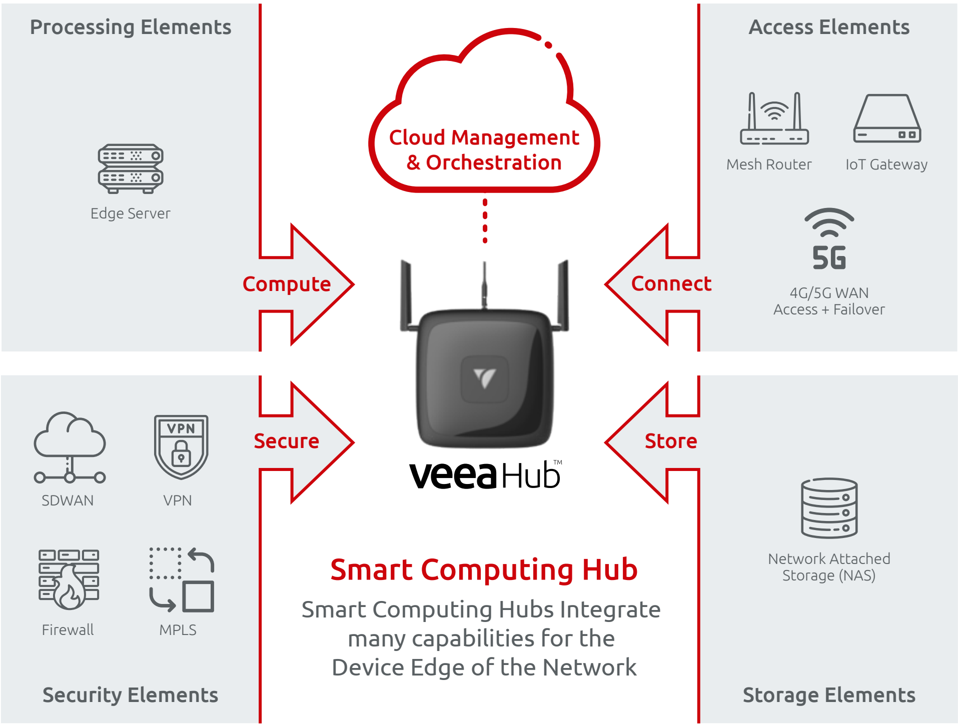
23% are unsure of what security protocols are on the device they are using the most.

Morphisec

Secure Access Enhanced by VeeaHub®

The vTPN Security Service is underpinned by Veea's innovative VeeaHub Smart Computing Hub™, a discreet access device which acts as an intelligent secure gateway for the remote user's location. Your network and all of your user's devices are protected, simply by connecting through their VeeaHub.

VeeaHubs combine secure wired and wireless connectivity, including Wi-Fi, Ethernet, and wireless broadband, offering an integrated, cost-effective, easily deployed secure access-point for unparalleled flexibility and management simplicity. As an additional benefit, IT can use VeeaHub's processing capability to support other IT applications for their remote users, while deploying and managing these new services from a central control portal.



Smart Computing Hub

Smart Computing Hubs Integrate many capabilities for the Device Edge of the Network

Simplicity Redefined

Work-from-home IT security solutions need to be simple to be effective. The vTPN Security Service is simple for users, simple to configure, and simple to manage.

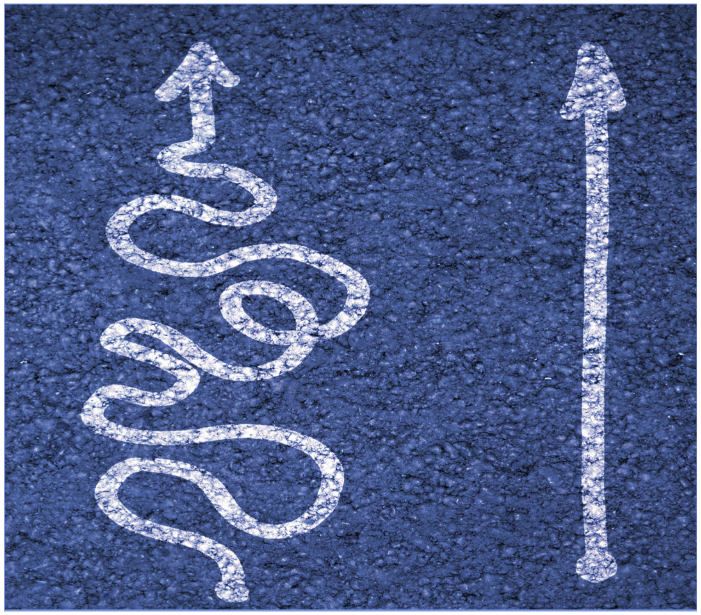
End-User Simplicity – VeeaHubs with the vTPN Security Service pre-installed ship directly to end-user locations. Remote users unbox and connect the VeeaHub to their local broadband or cellular WAN link. It is then ready to use.

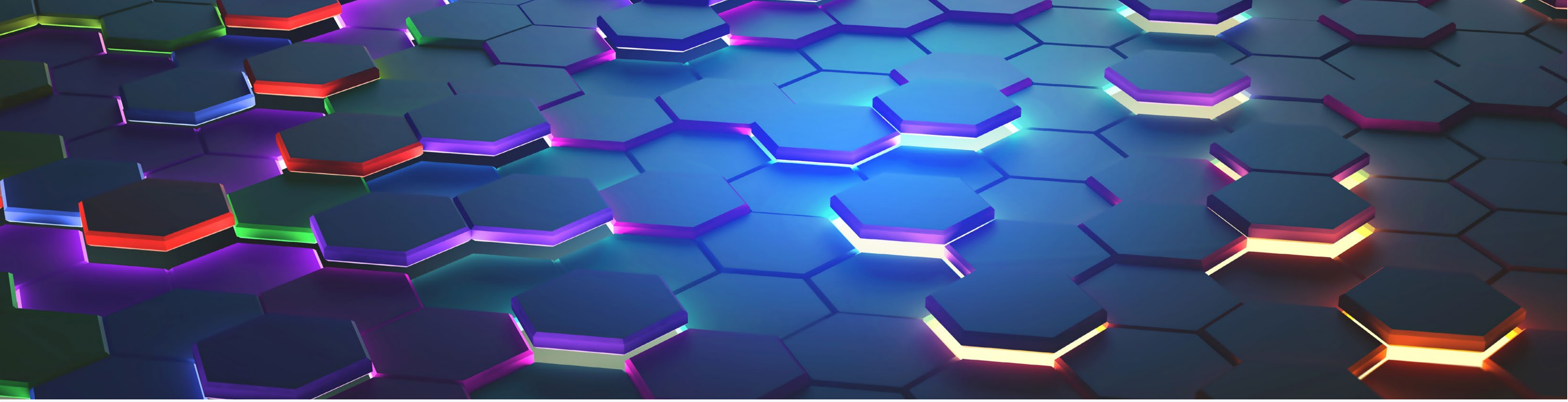
Security Beyond Passwords – The vTPN Security Service is endpoint-aware. Unlike most VPN endpoint software that just requires users to enter a username and password to use the service, vTPN's control elements know which devices and VeeaHubs can access the enterprise network – and which ones can't. The vTPN Security Service will not allow data from an unregistered device to access your network. Hackers cannot simply steal your remote user's credentials, and then access your network from their own device.

Configuration Simplicity – The Veea Control Center is a one-stop, unified management portal for VeeaHubs and the vTPN Security Service. With the Veea Control Center's intuitive Graphical User Interface (GUI), you can easily:

- Configure and manage your VeeaHub and vTPN Service elements
- Define access control, whitelist, blacklist and user security services
- Review system security status, and take action as necessary
- Access help, tutorials, service documentation, and more

Operational Simplicity – The Veea Control Center™ also provides a vTPN Security Service dashboard to provide an overview of the state of security for all of your remote worker endpoints. You can monitor and manage vTPN Service actions, view critical data charts, security alerts, and trends, all in a single dashboard. Receive notifications of security issues based on your preferences and understand the attack environment you are facing.





✓ Try Security Simplified – for Free!
Powerful security does not need to be complicated or require up-front fees.
Experience the vTPN Security Service at no charge through our 30-day trial.
Don't Fall Victim to Ransomware. Learn more at https://go.veea.com/vtpnfreetrial

About Veea

The Veea Edge Platform™ provides everything organizations need to quickly and easily tap into the power and benefits of Edge Computing. VeeaHub Smart Computing Hub connects to form an elastic, scalable, easily deployed, and managed connectivity and computation mesh. Veea Edge Services use this mesh to address common edge application needs. And Veea Developer Tools accelerate the deployment of our partners' and customers' edge and IoT solutions. Veea is blazing the path to new levels of integration, performance, and value at the network edge, resulting in operational simplicity, lower cost, and greater user satisfaction. For more information, visit https://www.veea.com and follow Veea on LinkedIn and Twitter.

Intelligently Connected™

Veea, Inc.
164 E 83rd Street
New York, NY, 10028
info@veea.com

EB-RA-002-0921

veea™