BUSINESS WHITE PAPER

# Simple, Secure Connectivity and Access for Home-based Workers

The future workplace includes a permanent and significant home-based workforce element. During the pandemic, many companies and employees realized the benefits of working from home. However, the supporting technology infrastructure that many companies had been using prior to the pandemic was not designed for a large-scale remote workforce. As a result, companies struggled to keep their systems running as the demand rose, and security sometimes took a back seat to productivity. That no longer need be the case.

In this white paper, you will learn about a simple, secure technology infrastructure that supports both employers and home-based remote workers and is reliable, scalable, and cost-sensitive.

veea™

## A Catalyst for Permanent Change

**It's a sobering truth that Covid-19 caught most businesses unprepared for a fully remote workforce. What had been a small percentage of home-based remote workers, suddenly became the majority of the workforce.**

As workers were forced to move their office space home, their supporting infrastructure changed. Many leveraged their existing home networks—often shared with other family members who were working, attending school zoom sessions, streaming video, or gaming. The Internet connection that had previously been suitable was suddenly unreliable and inadequate. Workers could not easily maintain reliable connections to some company resources. And, IT teams worldwide—suddenly remote themselves—had to address these issues quickly, often with what were expected to be quick, temporary solutions.

Security vulnerabilities became evident and widespread. Unsecured access to cloud applications, personal devices with weak passwords, and connectivity across a patchwork of secured and nonsecured networks exacerbated the already serious problem of cyber-attacks on data as it traversed networks ("data-in-motion"). As digital information moved between locations within or between computer systems, cyber-attacks occurred. Attackers hit data-inmotion at its most vulnerable points.

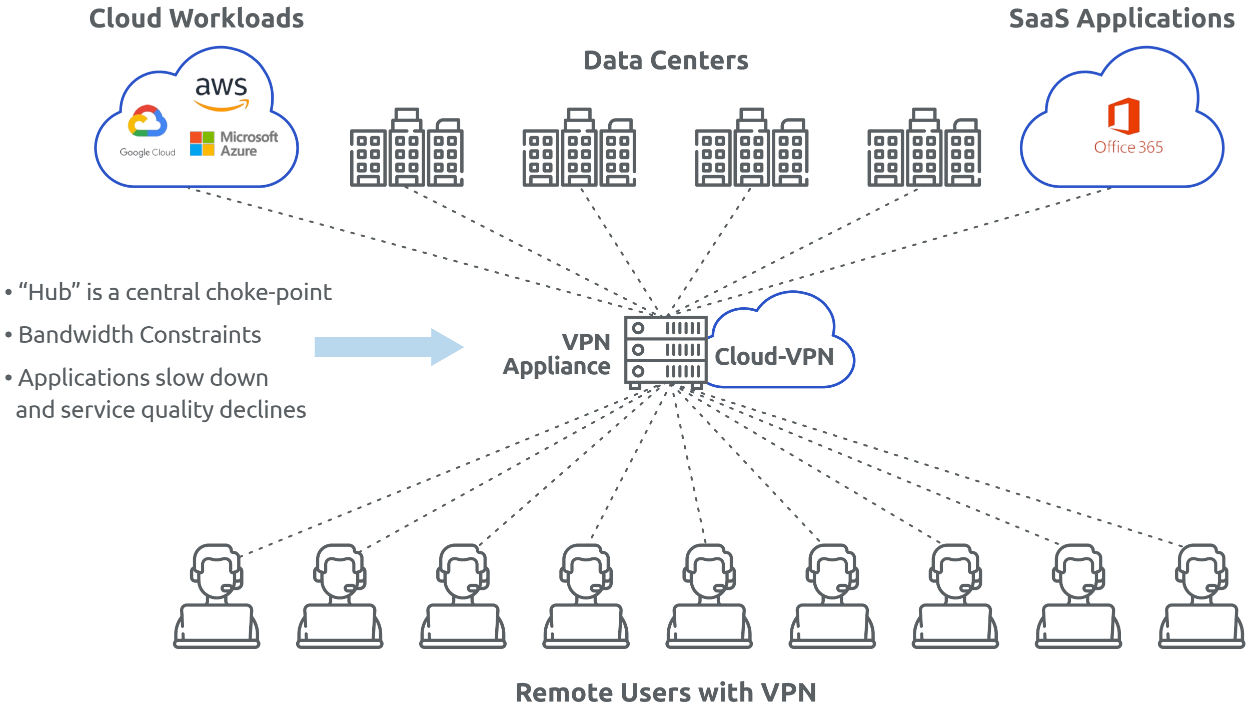
**Businesses need to ask themselves the hard questions:**

- How do we get business applications and data into the hands of the people who need them?
- How do we scale our remote solutions to serve the majority of employees—not just a few?
- Can our existing virtual private network (VPN) solution support this remote workforce?
- How do we protect business communications and sensitive data when many are working outside the safety of our network firewall?
- How do we manage this new distributed workforce model?

# The Remote-Enabling Technology Infrastructure

The new workplace paradigm requires a remote-enabling technology infrastructure that is flexible and scalable, yet simple to deploy cost-efficiently. Since this infrastructure will support a more permanent home-based workforce, it must meet the expectations of workers who are accustomed to an in-office IT support experience.

For years, businesses have been told that VPNs create a secure, private tunnel that allows communications and data to traverse safely over public, non-secure networks. This is, in fact, only partly true. As cyber criminals have become more sophisticated, they have exposed VPN security vulnerabilities, resulting in some very high-visibility data breaches and attacks. Unless businesses and their users are vigilant about consistently updating their VPN software, encryption protocols can become outdated and prone to attack. Also, VPNs don't inspect and filter incoming and outgoing traffic, which allows some security threats to slip through. VPNs typically require manual, high-touch administration, which introduces the element of human error into the security equation.



> *"...inspecting all traffic is a must for drastically reducing risk when squaring up against ransomware."*
>
> Google Transparency Report

# Smart Computing Hubs and the vTPN™ Security Service

## A Simple and Secure Solution

### The Smart Computing Hub at Home

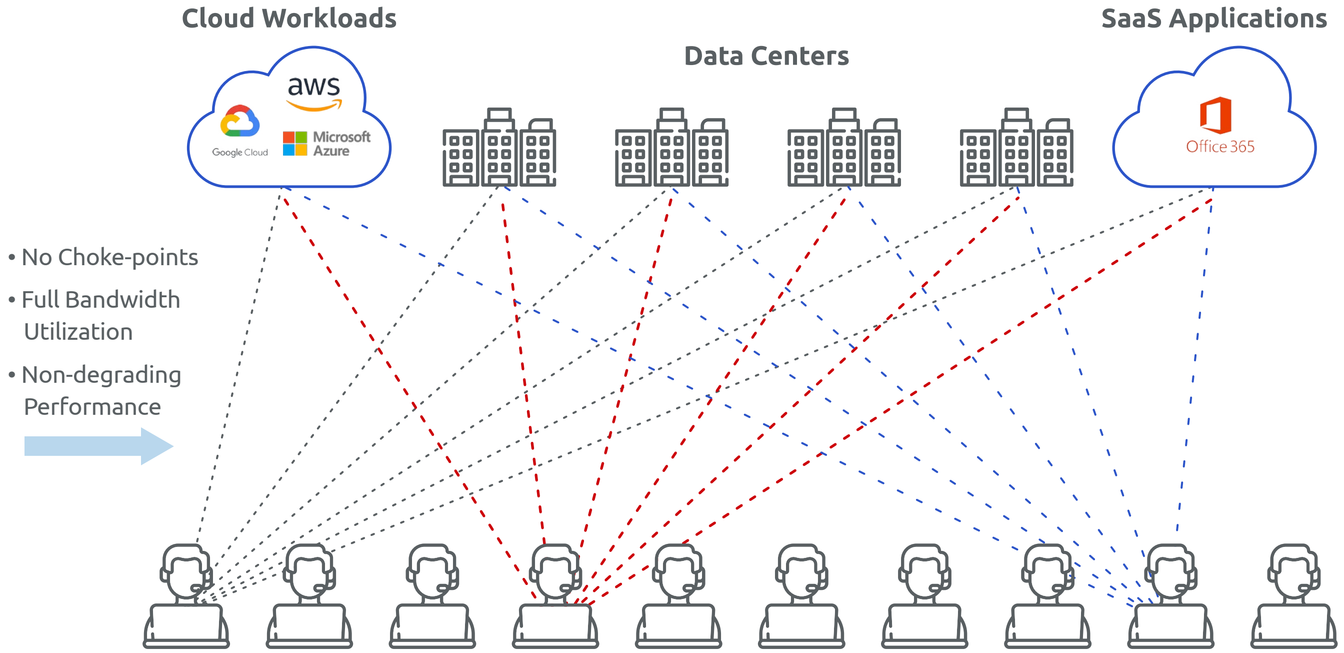
The VeeaHub is a simple, enterprise-grade connectivity solution designed to support home-based remote workers. It provides, protected Wi-Fi, Ethernet and optional wireless broadband connectivity separate from their personal broadband connectivity solutions, supports company-issued devices and Bring-Your-Own-Devices (BYODs), enables remote access to workplace desktop computers, and eliminates the cost and performance challenges experienced with traditional VPN solutions.

### The vTPN Security Service

Having robust connectivity isn't enough for your home-based remote workers. Security is paramount and businesses need to provide the same—or better—security to employees at home as they have in the office. This is easier said than done.

A full stack security solution, the vTPN Security Service is comprehensive so as to enable secure end-to-end remote access. For a distributed workforce, vTPN Service components are deployed at your user endpoints and at key network points in the cloud or enterprise. vTPN NetEdgeConnect software runs on VeeaHubs in remote workers' homes, and vTPN CarrierEdge or CloudEdge software is deployed in the cloud or on servers in enterprise data centers.

As a cloud-based security service, the vTPN Service inspects all traffic for threat potential. It maintains real-time data on threat vectors and user privileges to ensure secure access to application and resources in public and private clouds as well as corporate locations.



The vTPN Service protects against ransomware, malware, viruses, spyware, DDOS attacks, and more with fully integrated, 'always on' protection against data-in-motion threats—no matter if they originate outside or inside your environment.

### 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

> *"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

# A Winning Combination from Setup to Dashboards

**Setup is Simple.** The VeeaHub arrives pre-configured so that it can be deployed quickly by the home-based worker—unbox, connect, and use.

## 1 | Unbox

VeeaHub® ships with the vTPN Service pre-configured.

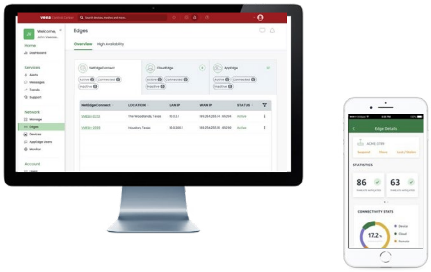
## 2 | Connect

Connect the VeeaHub to your local broadband and/or cellular WAN links.

## 3 | Use

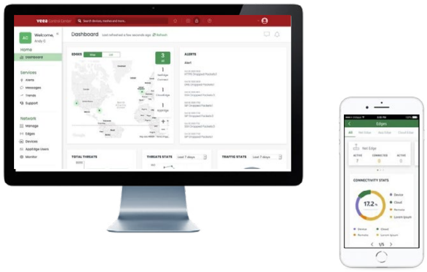
The VeeHub will be ready to go and use.

**Configuration is Simple.** Once the device has been setup in the home, the IT team can remotely activate, monitor, and manage the device.



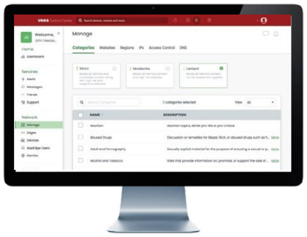
## 1 | Activate

A simple, unified interface manages your VeeaHubs and other vTPN Service elements.



## 2 | Monitor

Monitor your network with an intuitive graphical user interface and display critical data charts, security alerts, and trends in a single dashboard.



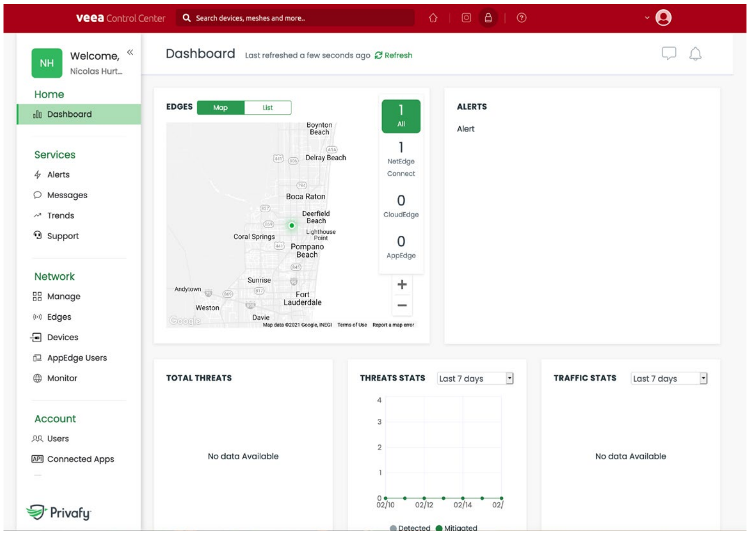
## 3 | Manage

Express your access policies and enforce them from one unified portal to all your locations, mobile devices, and cloud apps.

**No On-site IT Required.** Because the vTPN Service is cloud-based, all security management tasks can be performed remotely through a secure Internet connection. Encryption key management, policy updates, and software patches are all done automatically. The vTPN Service is easier to deploy, manage, maintain, and scale than a traditional VPN.

**Full-Stack Security.** The vTPN Service is comprehensive for protection against data-in-motion threats, DoS attacks, data theft, and ransomware. More than a VPN, the vTPN Service offers multi-layer security for your network and every endpoint and user.

**Dashboards Support Operations.** IT can get the big picture with vTPN Service dashboard. You can establish whitelists and blacklists for your network and users, receive notifications, 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
+1 (855) 488-7332

WP-RA-001-0921