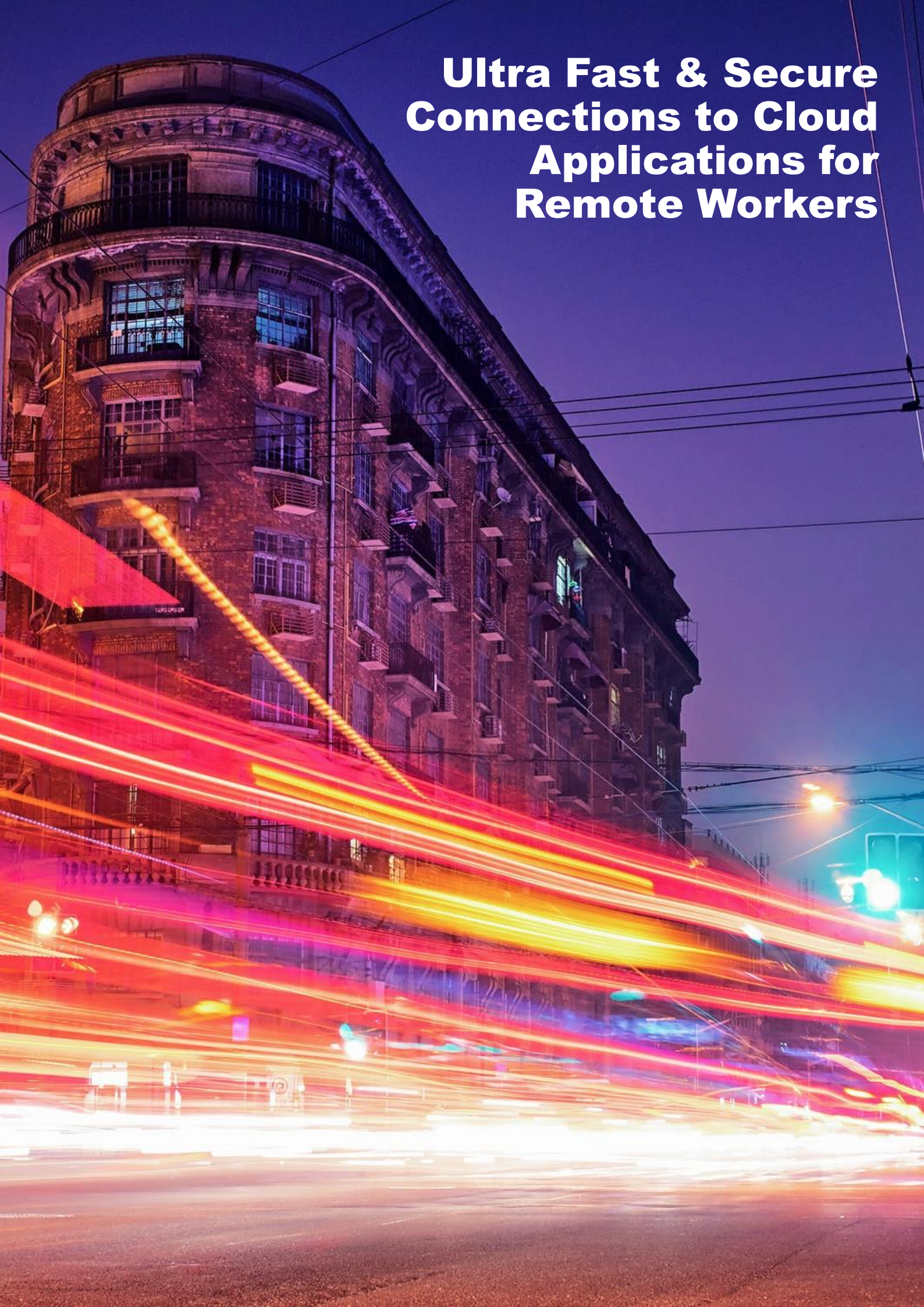


Ultra Fast & Secure Connections to Cloud Applications for Remote Workers

Connect Users Directly to Cloud Applications With iboss Cloud

Cloud applications require a lot of bandwidth to enable users to be productive and have a great experience.

Content sharing sites, online meeting apps like Zoom, and Microsoft 365 require fast connections as data is exchanged between users and those applications in the cloud.

Ensuring compliant and secure connections to the cloud is also a requirement to prevent malware and data loss. To make things challenging, users have all gone remote but fast and secure connections to these applications is still required.

If data is being sent through a VPN for remote work, slow connections are almost guaranteed as the data overwhelms VPN infrastructure, data center bandwidth and on-prem network security infrastructure.

The loss in productivity and poor end-user experience from remote workers results in exponential losses to the organization as work comes to screeching halt.

Connect Users Directly to Cloud Applications With iboss Cloud

The iboss cloud platform can alleviate this problem immediately by offloading all cloud traffic from the VPN and sending it directly to the applications in the cloud.

This includes offloading Microsoft 365 traffic, online meeting applications, G-Suite and virtually all cloud and Internet bound traffic through the iboss cloud security service.

The iboss cloud platform ensures compliance, malware defense and data loss prevention are applied to all connections, without having to send those connections through slow and bottlenecked office connections.

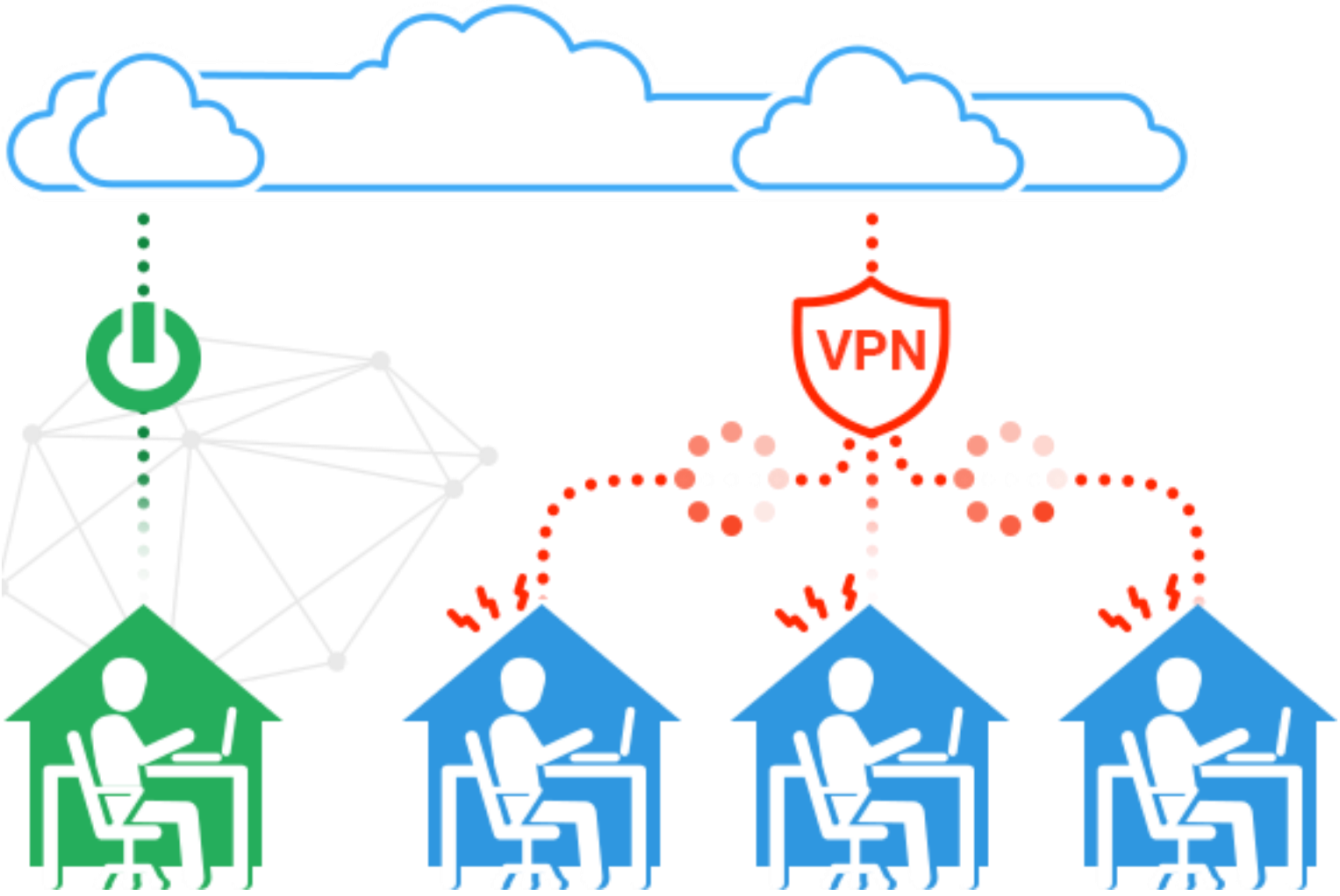
The Problem

The applications users need live in the cloud.

Virtually all applications have moved to the cloud or will be there soon. However, the connections between users and those applications may still be going through the office or data center through VPNs.

Why is network data from end users to cloud applications going through the corporate network if those users are remote and the applications they are accessing are not in the office?

The typical answer is that this is done to ensure compliance, malware defense, data loss prevention and visibility remains intact as users work remote and connect to cloud resources.

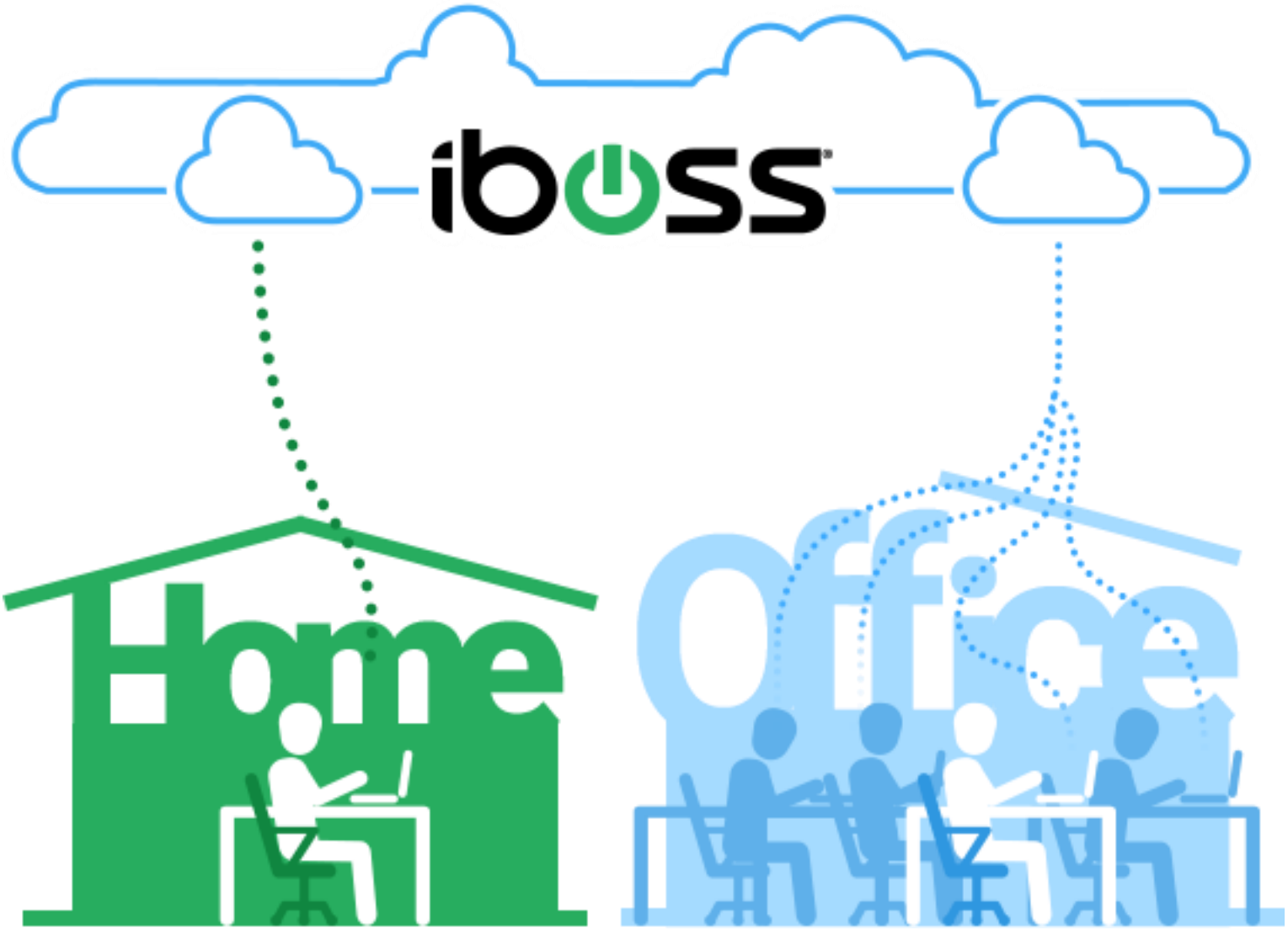


However, remote workers typically have a lot of accessible bandwidth at a very low consumer price.

When you multiply the number of remote works and the amount of bandwidth available to each, the amount of total bandwidth being sent through the VPN and on-prem proxy appliances is staggering.

There is no amount of network security proxies, VPN infrastructure or bandwidth that an organization can purchase that can handle the type of load required to secure the volume of bandwidth from all of the remote workers.

And HTTPS encrypted traffic makes things worse as that traffic must be decrypted in order to be inspected, increasing appliance purchases even further.

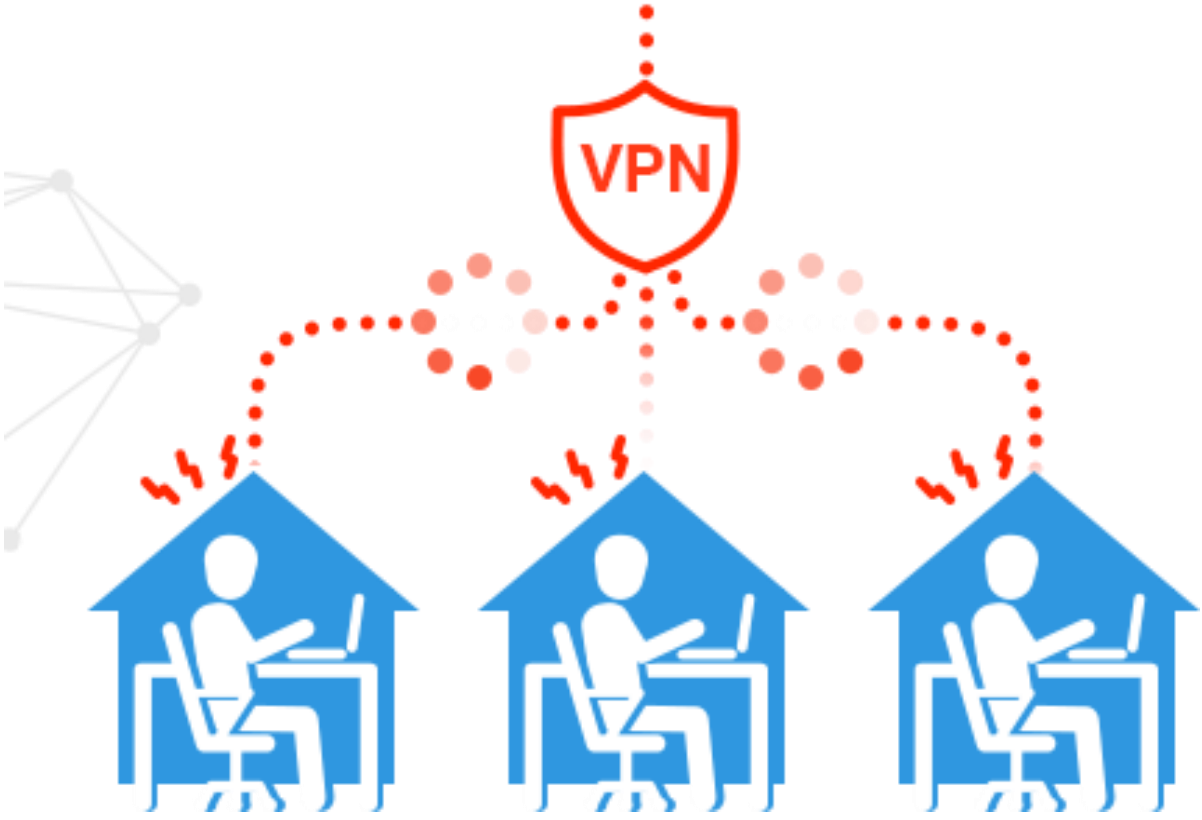


Typical Complaints and Challenges

Slow connections to cloud applications

Remote workers complaining that the VPN is slow or they cannot connect to the VPN leaving them unable to work on Microsoft 365 or connect to online meetings

Remote workers unable to connect to cloud applications due to slow or poor connections through the corporate data center



How the Solution Works

The iboss cloud platform runs in the cloud.

Users are connected directly through the iboss cloud platform while they access cloud applications like Microsoft 365, Teams, Zoom, content sharing applications and other online resources.

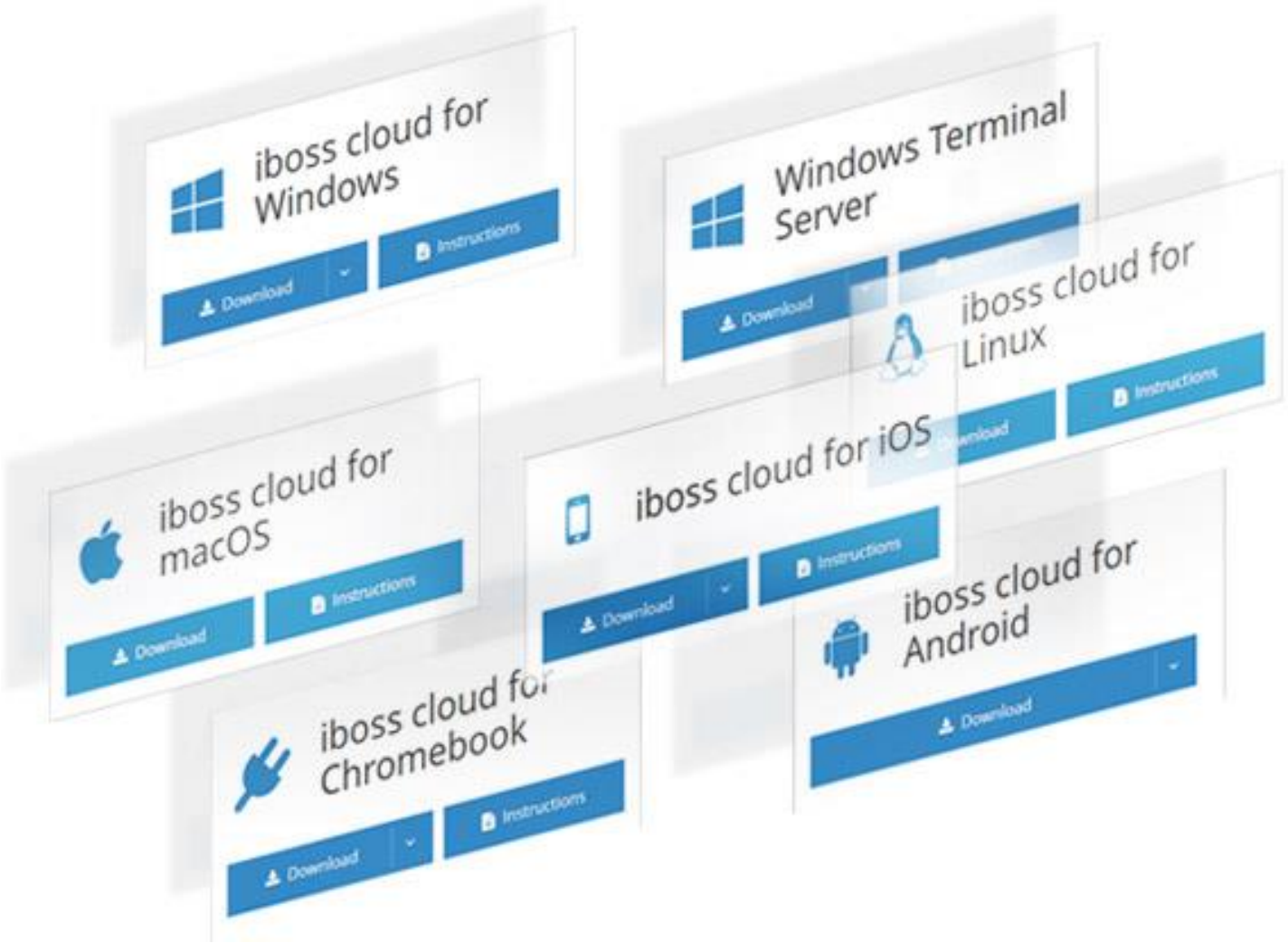
As the connections go through the iboss cloud platform, the network data is scanned for compliance, malware defense and data loss to ensure security and visibility is applied at all times.

How the Solution Works

The iboss platform includes agents for virtually every operating system and can also be pushed by MDM.

User connections to all cloud applications will immediately improve as there are no restrictions in the amount of bandwidth the iboss cloud platform can handle.

The agent also takes care of all technical details automatically, such as installing the root MITM decryption certificate to inspect all HTTPS traffic.



Instant Benefits and Savings

Users connected directly to applications, improves productivity and end user experience instantly.

In addition, the elimination of proxy and other network security appliances results in the reduction of the data center footprint and large reductions in infrastructure costs.

The savings continue as the iboss cloud platform eliminates the need to purchase more network proxies or VPN infrastructure as remote worker cloud application use and bandwidth increases over time.

The IT team no longer worry about bandwidth issues and poor connectivity.

First Response are a cybersecurity, digital forensics and incident response company headquartered in London.

Contact our sales team for further information on the iboss solution or for detail on the wider services and solutions we provide:

First-response.co.uk/
keith.towndrow@first-response.co.uk
+44 20 7193 4905

first response