

Security for Work from Home Employees

We're in a time of rapid change for our IT environments. As companies shift from working in an office within their controlled network to working from home, many are finding that the architectures they have in place aren't ready for the scalability and security challenges of a decentralized workforce.



Connect With Us



SOLUTION BRIEF

There are three prominent scenarios created by this shift that have an impact on security posture:

- 1. The internet is accessed directly, without a VPN:**
Most VPN deployments aren't ready to scale to an entire workforce routing traffic through them. Slowdowns and outages can cause users to turn off their VPN. Some may not be licensed for the entire workforce. In each scenario, devices will access the internet directly without the defense in depth of a managed network.
- 2. Data going to cloud services no longer routes through the corporate network:** There has been a [massive increase in the use of cloud-based tools](#) to support meetings and collaboration for decentralized teams. With direct internet accesses, data sent to the cloud falls out of visibility and becomes vulnerable. Sharing within the cloud and to external parties also falls outside of visibility and control.
- 3. Unprotected devices are being used for work:**
Some organizations may be asking employees to use their personal laptops for work at home. Others are issuing new managed laptops that need to ramp up with existing endpoint security.

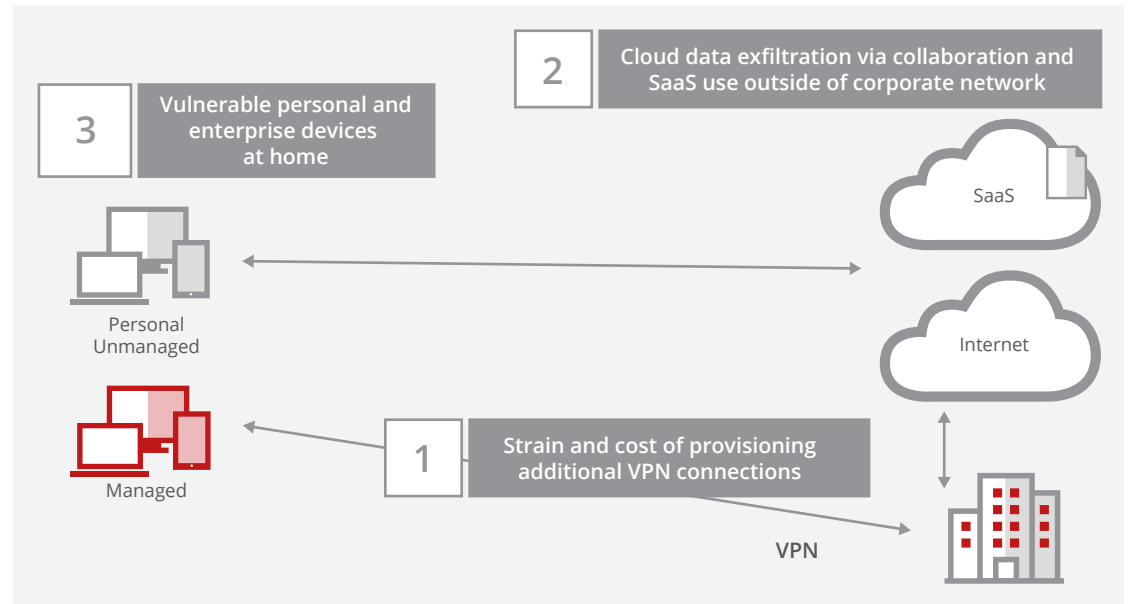


Figure 1. How an increase in employees working from home impacts security posture.

SOLUTION BRIEF

For many, existing security investments can be slightly augmented or scaled to cover these use cases. Others may need to quickly add capabilities. Let's discuss how, beginning with a set of requirements. To enable a secure and productive work from home environment, we recommend that:

1. Corporate devices are protected against web-based threats without routing through VPN.
2. Employees can connect to sanctioned cloud services from their corporate devices without using their VPN.
3. Cloud services have device checks, data controls, and are protected against attackers who can access SaaS accounts over the internet.
4. Corporate devices have complete endpoint threat prevention, detection, and response in place.
5. Employees can use their personal devices to access corporate SaaS applications, with conditional access to sensitive data in the cloud.

To fulfill these requirements for securing remote employees, enterprises can deploy the following security capabilities.

Enable Direct-to-Web Browsing and Cloud Access

To regain the defense in depth of on-premises web security, companies can deploy McAfee® [MVISION Unified Cloud Edge](#), which uses a cloud-based secure web gateway to add access control, advanced malware prevention, and data loss prevention to any internet connection from a managed device. This is built for large enterprises, with an average service availability of 99.999%.¹ Managed devices can connect to the cloud-based secure web gateway at home and from any other internet connection worldwide. Existing customers of McAfee® Web Gateway can add this cloud service to create a hybrid deployment for their web security.

Protect Data on Endpoints and in Cloud Services

Outside of a corporate network, protecting data requires new control points at the source of data itself. [Data Loss Prevention](#) on a managed endpoint will prevent sensitive and regulated data from leaving your visibility to a USB device or external media.

For the increase in data going to cloud services from employees collaborating remotely, a [cloud access security broker \(CASB\)](#) provides the most comprehensive security. CASBs enable visibility and control over data entering, moving within, and attempting to leave cloud services, along with threat prevention and control over Shadow IT.

SOLUTION BRIEF

Add Endpoint Security to Unprotected Managed Devices

New managed devices issued to employees can quickly get up to speed with the rest of the enterprise's [endpoint security](#) in two ways. First, any McAfee® Endpoint Security customer with a subscription license can deploy the solution to five devices per user and can do so immediately. For new users, additional McAfee Endpoint Security licenses can be added to scale out.

iOS and Android devices used to conduct business can be protected by McAfee® [MVISION Mobile](#), which provides real-time, machine learning-based protection against device, network, phishing, and malicious app attacks.

Add Endpoint Security to Unprotected Personal Devices

Personal devices are, by definition, not managed by your IT team and require individual end users to install and manage their own security. The McAfee® Home Use program allows companies to purchase McAfee® LiveSafe™ for employees to use independently on their personal devices. Contact homeuse@mcafee.com to get started.

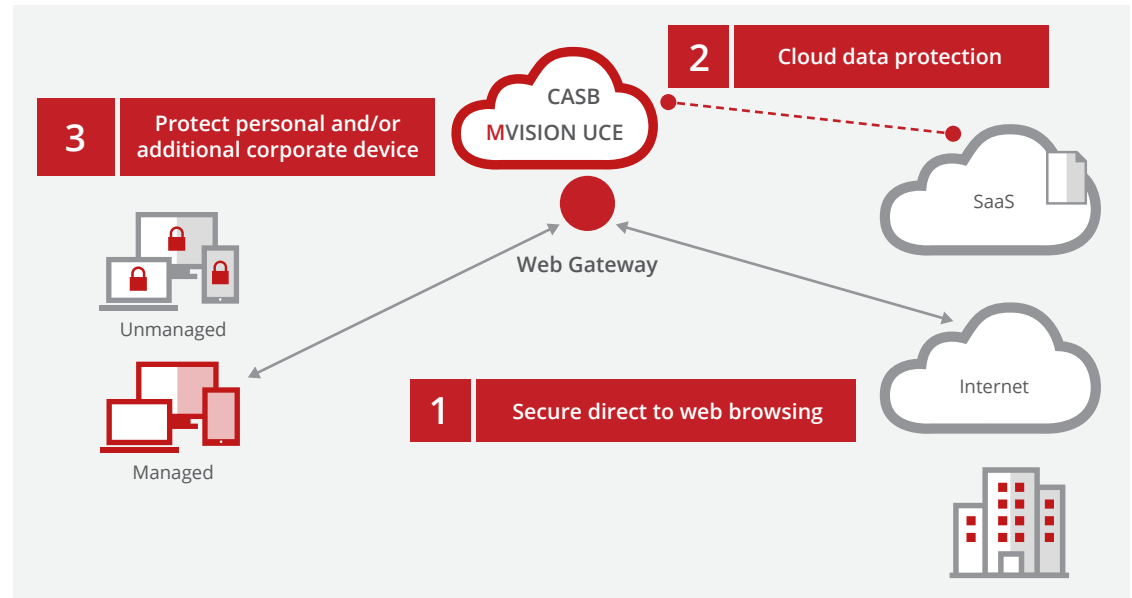


Figure 2. How McAfee Endpoint Security, McAfee Web Security, and CASB solve the challenges of securing work from home employees.

For more information on these solutions please visit mcafee.com/workfromhome.

1. Measured April 2020 on a 90-day rolling basis. Current status can be found here: <https://trust.mcafee.com/web/> and details on the calculation found here: https://trust.mcafee.com/saas_sla.pdf.



2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2020 McAfee, LLC. 4454_0420 APRIL 2020