Solving the Challenges of Modern Remote Access

Published 25 March 2020 - ID G00722990 - 8 min read

By Analysts Rob Smith, Steve Riley, Jeremy D'Hoinne, Nathan Hill

Initiatives:Infrastructure Security **and 2 more**

Remote access VPN was thought of as a dying technology until COVID-19 changed the way people work. This research offers guidance, including a decision tree, for security and risk management leaders to solve the challenges of quickly scaling large-scale modern remote access.

Additional Perspectives

- Invest Implications: Solving the Challenges of Modern Remote Access
  (30 March 2020)

Overview

Key Findings

- Most organizations only have capacity and licenses to handle a small subset of users and are not prepared to enable all employees for remote work during critical events such as COVID-19.
- Always-on VPNs are being used for all of a user's connections and resource consumption, even when some users only need access to cloud-based applications and data.
- Deployed technology is often out of date and missing required licenses to support the entire organization.
- Organizations frequently lack required bandwidth needed to support all users working remotely simultaneously.

Recommendations

Security and risk management leaders tasked with infrastructure security and enabling remote access must:

- Determine user remote access requirements such as on-premises or cloud applications before choosing or deploying any product.
- Test products for scale to support critical unplanned events such as COVID-19.
- Evaluate the risks of enabling unknown devices previously not used in the organization, such as bring your own PC (BYOPC).

- Develop a usable remote work policy that has been agreed with all key stakeholders. If this is not possible due to time constraints, still consult counsel to verify it passes all local laws.

Analysis

Introduction

For over the past 20 years, enterprises have relied on VPN technologies to enable remote access to applications and data. Over time, users' dependency on access to the corporate network has diminished as enterprises have transitioned to cloud-based applications.

However, many enterprises still route all traffic through the corporate network before delivering to any cloud-based application, resulting in performance degradation of sufficient hindrance that users seek ways to bypass security and instead access the applications directly. At the same time, few enterprises are prepared to enable remote access for all employees at once to support remote work during emergencies such as the COVID-19 crisis. Solutions such as a cloud access security broker (CASB) or zero trust network access (ZTNA) could resolve these problems. Alternatively, users could be allowed to securely access those applications outside of the corporate network; but where a CASB is used, additional corporate controls can be enforced by using an access management (AM) tool. Also note that Gartner strongly encourages all enterprises/SRM leaders to pilot and deploy multifactor authentication (MFA) for any kind of remote access; phone-as-a-token authentication is very suitable here.

This research offers technology and policy guidance for deploying modern high-volume remote access.

Know Your Requirements Before Looking at Technology

Frequently, Gartner sees organizations buying and deploying products without first knowing what the exact requirements are of the end users. This leads to poor performance and even potential security vulnerabilities. Four variables should be first considered when defining any use case (see Figure 1):

1. **Who are the users and what is their job function?** All users are not equal. Some users, such as executives or mission-critical employees as well as those who have intense data analysis needs, may require more bandwidth than an average user who simply checks email.

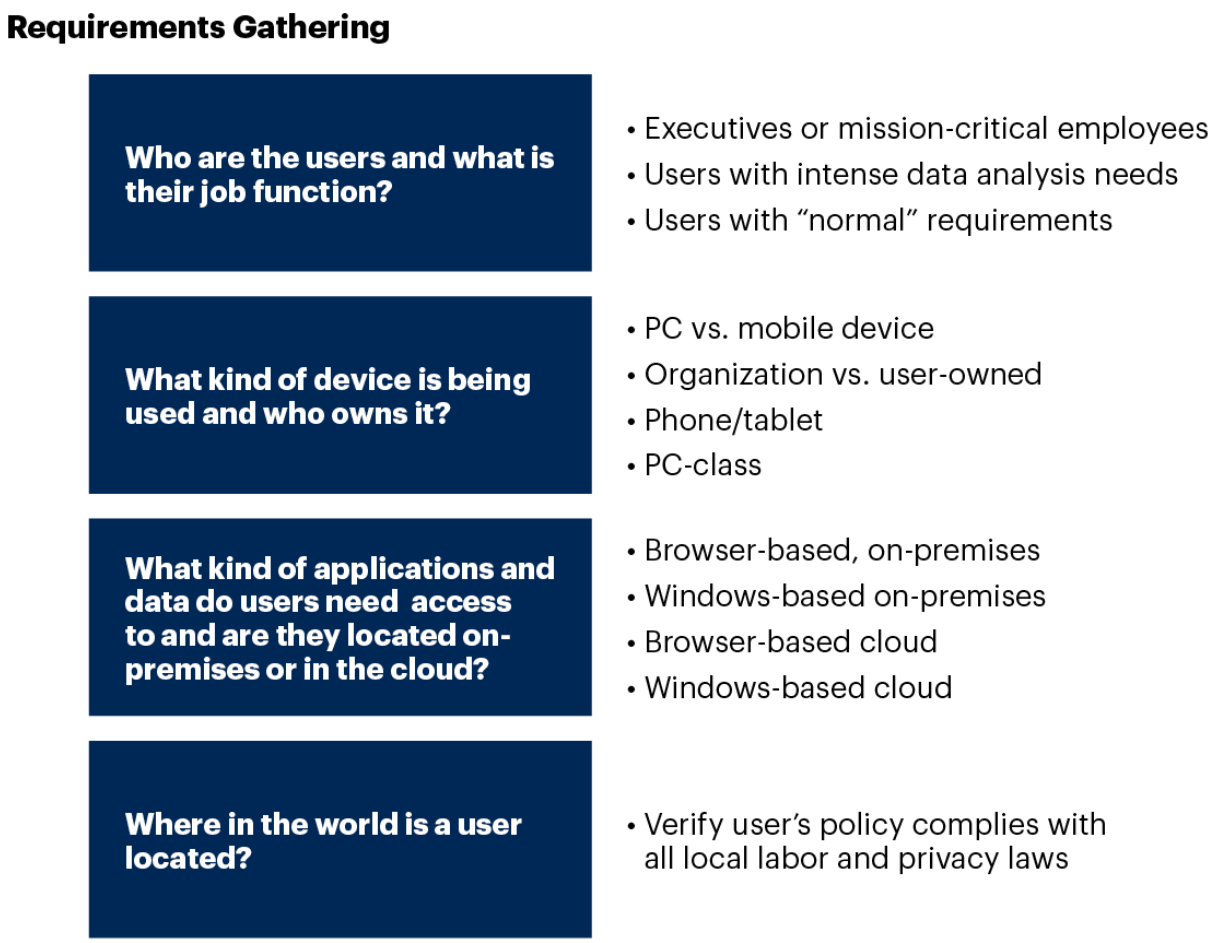
2. **What kind of device is being used and who owns it?** Usability and security vary widely across the universe of devices. A corporate-owned PC is much easier to secure than a personally owned smartphone.

3. **What kind of applications and data do users need to access and are these applications and data located on-premises or in the cloud?** For example, for users who only need to use dedicated SaaS applications, having an always-on VPN to the corporate network would deliver a

poorer performance versus using an access management tool, or a CASB with (or without) an AM tool.

4. **Where in the world is a user located?** A wide array of data security, labor, and privacy laws spread across countries and local jurisdictions complicates offline data storage choices.

Figure 1. Requirements Gathering



Source: Gartner
722990_C

Once use cases are determined based on the four variables, users can be put into different service offerings such as cloud-only, remote user or highly regulated and secure. IT can then build the appropriate technology required to meet these use cases. See the Remote Access Solution Decision Tree section to assist in selecting the appropriate solution. It is important to note that most large enterprises will typically have at least two or three main use cases which other policy can be based from.

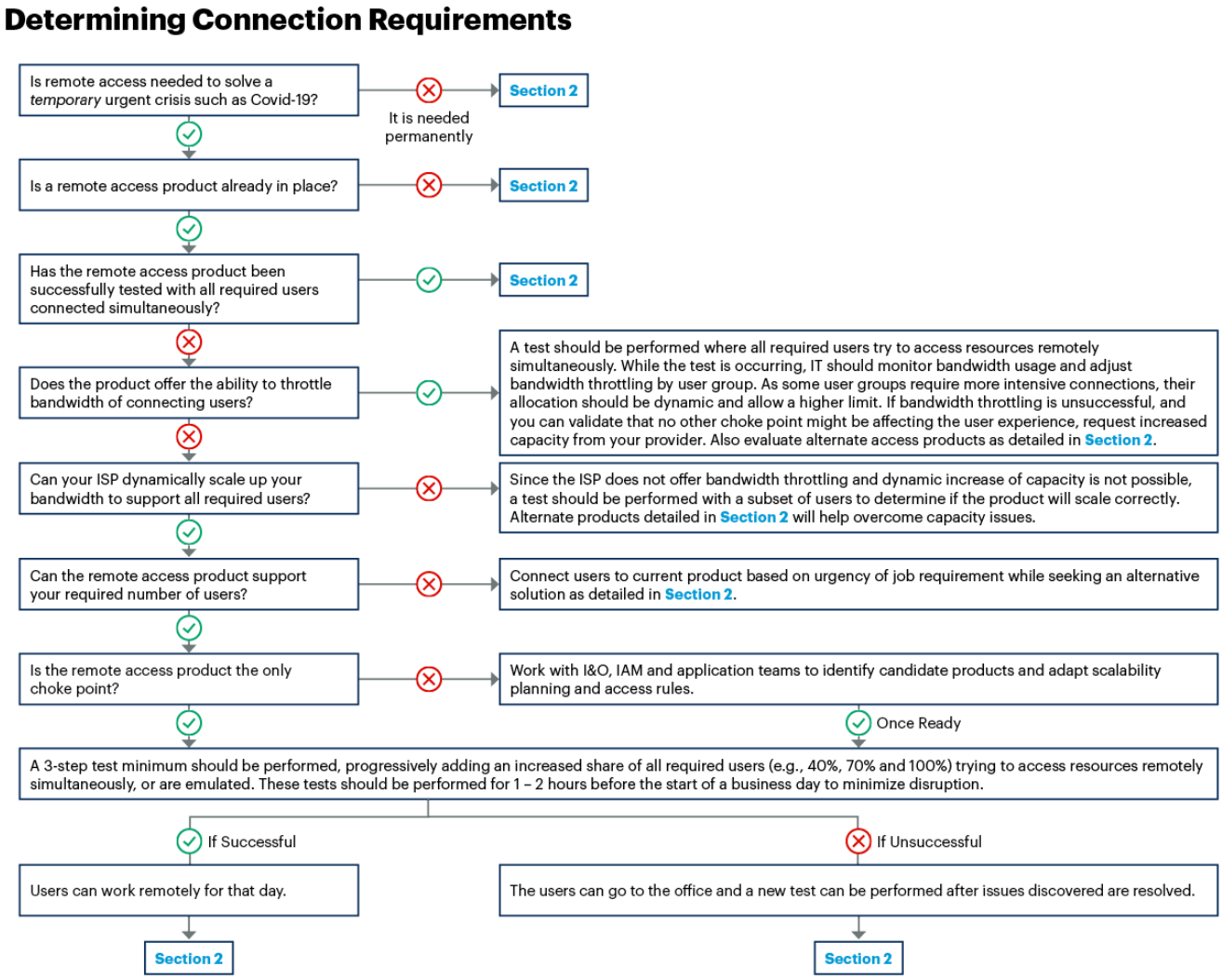
Remote Access Solution Decision Tree

The following decision tree will aid in purchasing and deployment decisions. Most organizations of large scale will require multiple products. These products will answer needs related to the user requirements previously defined.

Section 1 — Connection Requirements

Before evaluating individual remote technologies, it is important to understand the current status of any existing remote access deployment. Figure 2 offers a decision tree to help determine if a deployed product is usable in an urgent crisis such as Covid-19.

Figure 2. Determining Connection Requirements



Source: Gartner
722990_C

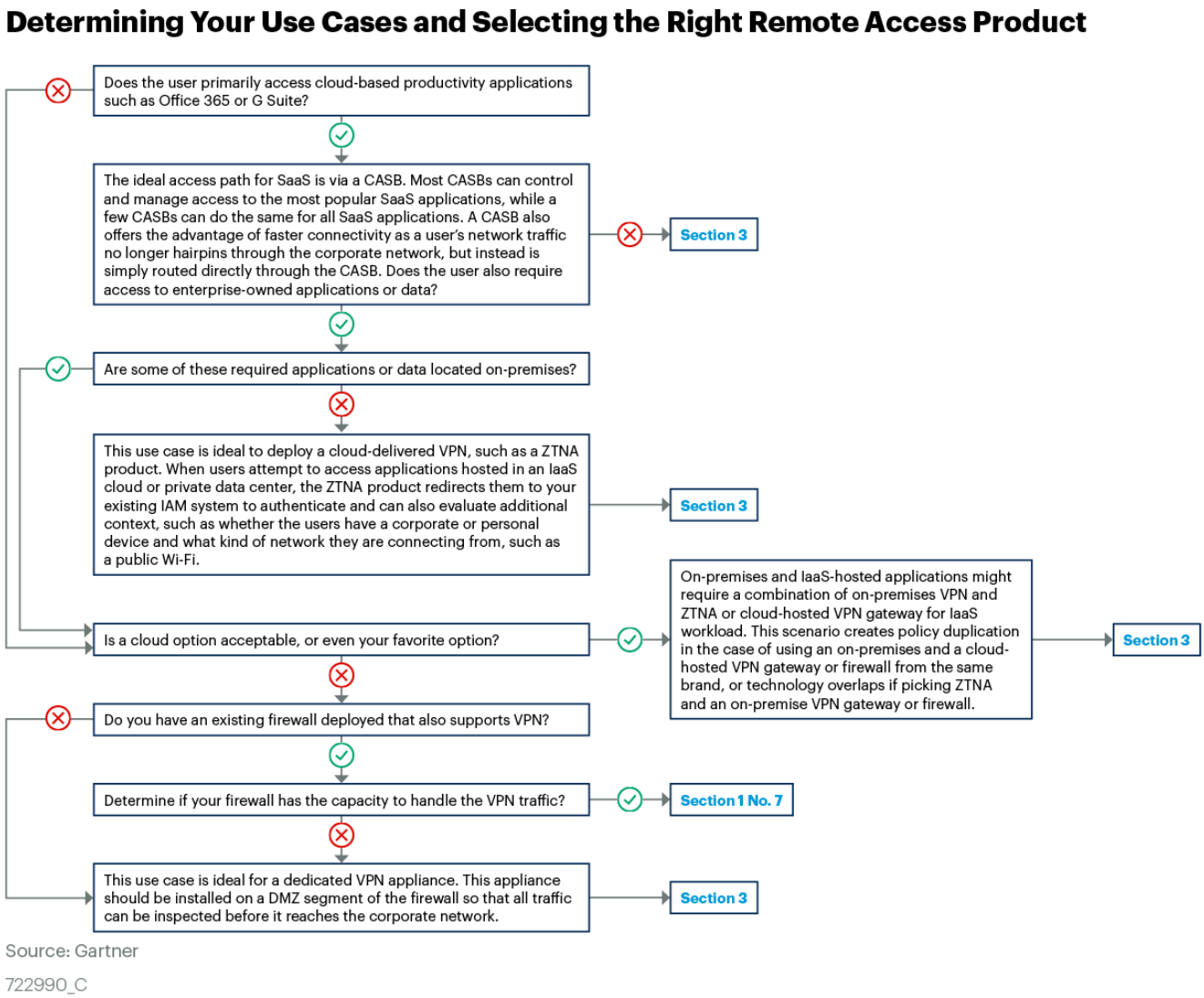
Section 2 — Determining Your Use Cases and Selecting the Right Remote Access Product

Even if there is an existing, workable product in place today, it still may not be optimal for providing the best experience for all users or with the scale required to support all in a crisis. The decision tree in Figure 3 will assist in selecting the right tool to meet the right use cases. As detailed previously, variables dictate the requirement to deploy multiple products. These include:

- Users' job functions
- Types of devices they need to use and who owns the device

- Applications and data they need to access and where that data is stored
- Geographic location of the user

Figure 3. Determining Your Use Cases and Selecting the Right Remote Access Product



Source: Gartner

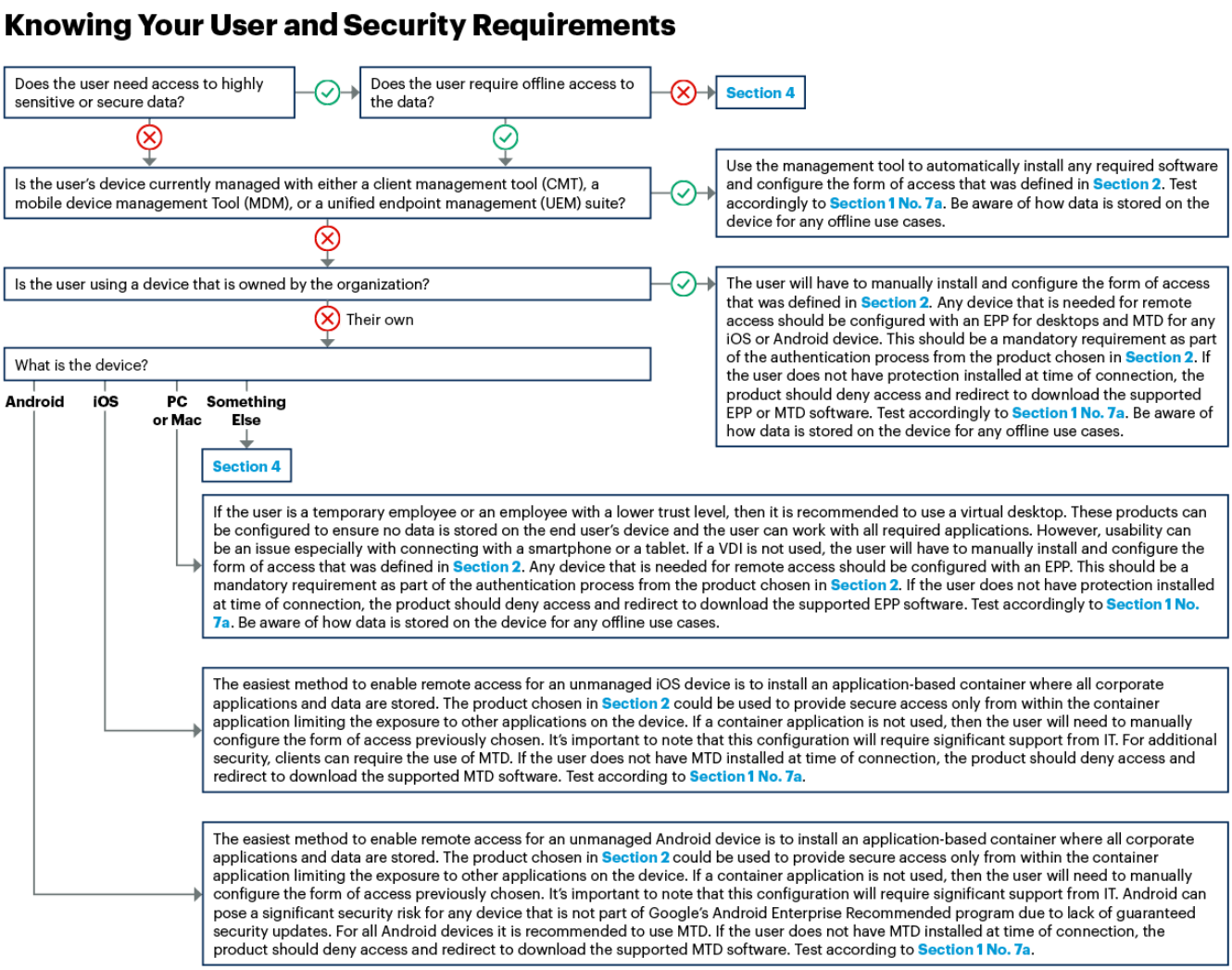
722990_C

For more information about VPN and possible VPN vendors, see "Market Guide for Secure Enterprise Communications." For more information about ZTNA and possible ZTNA vendors, see "Market Guide for Zero Trust Network Access." For more information about CASB and possible CASB vendors, see "Magic Quadrant for Cloud Access Security Brokers." For more information about access management and possible access management vendors, see "Magic Quadrant for Access Management." For more information about phone-as-a-token authentication and possible vendors, see "Technology Insight for Phone-as-a-Token Authentication." For more information about IaaS, see "Magic Quadrant for Cloud Infrastructure as a Service, Worldwide."

Section 3 — Knowing Your User and Security Requirements

Figure 4 details when and how to deploy different technologies based upon different use cases, device type and device ownership, while providing the appropriate level of security.

Figure 4. Knowing Your User and Security Requirements



Source: Gartner

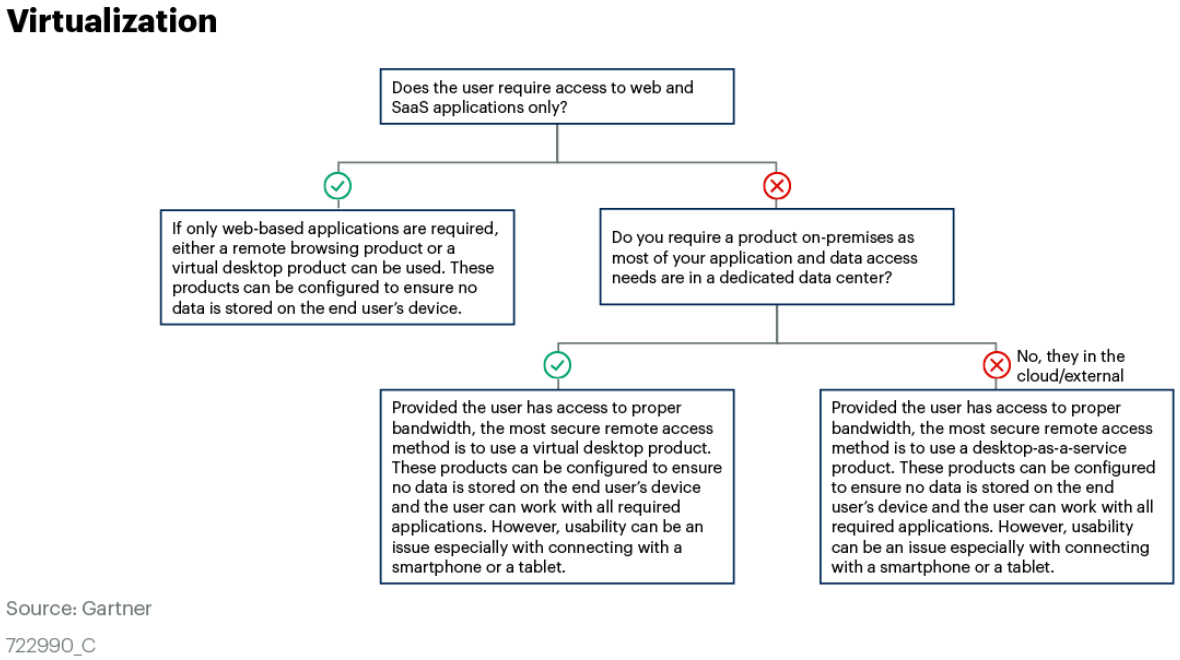
722990_C

For more information about endpoint protection platforms (EPPs) and possible EPP vendors, see "Magic Quadrant for Endpoint Protection Platforms." For more information about mobile threat defense (MTD) and potential MTD vendors, see "Market Guide for Mobile Threat Defense." For more information on how data should be stored and protected on devices for offline use cases, see "Market Guide for Information-Centric Endpoint and Mobile Protection." For more information about device management, see "Magic Quadrant for Unified Endpoint Management Tools." For details on Apple device security, see "iPhone and iPad Security FAQs." For details on Android security, see "When Android Is Secure Enough for the Enterprise." For details on Windows 10 security, see "Windows 10 Enhances Security."

Section 4 — Virtualization

If security requirements prohibit storing data on individual personal devices or if Windows applications must be run on non-Windows (or unknown) devices, virtualization is an ideal option. Figure 5 illustrates specific use cases.

Figure 5. Virtualization



Source: Gartner
722990_C

It is important to note that any virtual solution on a smartphone or tablet frequently suffers from poor usability, and any application needed should be redesigned to support the required devices when time is available to do so. For more information on selecting between virtual desktop infrastructure (VDI) and desktop as a service (DaaS), see "Physical, Virtual and Cloud Desktops: Is a Hybrid Approach Inevitable?" and "Market Guide for Desktop as a Service." See "Innovation Insight for Remote Browser Isolation" (archived) for more details on remote browsing when using web-based applications.

Remote Work Policy

After use cases and technology have been determined, IT can build an end-user policy document. This document should be approved by stakeholders including human resources, legal, security, compliance, labor unions/workers councils and executive leadership. Any policy document should be physically signed by the end user and not simply a click-through online agreement. The policy should also be written in simple local language, avoiding any legal terminology. If this is an urgent issue, the policy still should be vetted by legal counsel and employees should still physically sign the document as soon as possible. See "Toolkit: Remote Work Policies" and "Toolkit: Unified Endpoint Device Policy and Procedures Template" for assistance with policy creation.

Acronym Key and Glossary Terms

VPN	Virtual Private Network

ZTNA	Zero Trust Network Access
CASB	Cloud Access Security Broker
VDI	Virtual Desktop Infrastructure
DaaS	Desktop as a Service
IaaS	Infrastructure as a Service
EPP	Endpoint Protection Platforms
MTD	Mobile Threat Defense
UEM	Unified Endpoint Management
CMT	Client Management Tools
MDM	Mobile Device Management

Evidence

Evidence

COVID-19 is impacting bandwidth availability:

"Netflix to Limit Streaming Quality for European Subscribers to Preserve Bandwidth During Coronavirus Crisis," Deadline Hollywood.

Recommended by the Authors

Magic Quadrant for Cloud Access Security Brokers

Market Guide for Secure Enterprise Data Communications

Market Guide for Zero Trust Network Access

Magic Quadrant for Cloud Infrastructure as a Service, Worldwide

Market Guide for Information-Centric Endpoint and Mobile Protection

Market Guide for Mobile Threat Defense

Market Guide for Desktop as a Service

Physical, Virtual and Cloud Desktops: Is a Hybrid Approach Inevitable?

Toolkit: Remote Work Policies

Toolkit: Unified Endpoint Device Policy and Procedures Template

Recommended For You

Hype Cycle for Endpoint Security, 2019

Protecting Against 'Living Off the Land' Attacks

Critical Capabilities for Secure Web Gateways

Market Guide for Mobile Threat Defense

Magic Quadrant for Secure Web Gateways