

NO
1



The Remote Access Buyer's Guide for SMEs and Larger Organizations

BUYERS GUIDE

TABLE OF CONTENTS

The Importance of Remote Access for SMEs and Large Enterprises	03
Understanding Remote Access Needs	04
Key Reasons for Seeking Remote Access Solutions:	04
Critical Factors to Consider When Choosing Remote Access Software	05
Scalability	05
Security and Compliance	05
Performance	05
Compatibility	05
Support and Training	06
(A) Cloud vs. Direct Connectivity:	07
Direct Connections for Enterprises	07
Cloud Connections for Enhanced Scalability	07
Making the Right Choice for Your Enterprise	07
(B) Installed vs. On-Demand Access:	08
Installed Access	08
On-Demand Access	08
Strategic Consideration	09
(C) On-Premise Solutions	09
Enhanced Security and Compliance	09
Customization and Integration	09
Resource Considerations	10
Conclusion	10
Comparing Remote Access Solutions for Enterprises	11
Quick Product Feature Comparison	11
Evaluation Framework	13
Implementation and Best Practices	14
Get the Ultimate Buyer's Guide to Remote Access Toolkit	15

THE IMPORTANCE OF REMOTE ACCESS FOR SMES AND LARGE ENTERPRISES

Remote access software plays a vital role in maintaining productivity, security, and operational continuity for businesses of all sizes. It enables employees to connect to their office systems from anywhere, ensuring seamless workflows and collaboration, even in diverse geographical circumstances.

Selecting the right remote access solution is paramount; there's a lot at stake. The implications of choosing the wrong tool can significantly affect both functionality and security, leading to potential productivity losses and financial implications. While there are numerous basic remote access tools available, some are specifically designed for

Managed Service Providers (MSPs), focusing on remote support features. In contrast, all-in-one Remote Monitoring and Management (RMM) solutions cater primarily to IT needs, incorporating active monitoring alongside remote access. However, such solutions may not always provide the best user experience for remote work situations due to their complexity and larger commitments. Therefore, understanding the specific requirements of your business and the nuances of various offerings is essential to ensure a solution that effectively meets your needs as a large organisation.



UNDERSTANDING REMOTE ACCESS NEEDS

As large enterprises navigate the complexities of modern business operations, a clear understanding of their unique remote access requirements becomes essential. Key considerations include scalability, security, compliance, and efficient multi-site management.

Businesses face common challenges when implementing remote access solutions, such as ensuring robust security measures are in place, and managing a diverse IT environment, comprising various devices and operating systems.

Key Reasons for a Remote Access Solution:

Reducing Costs: Enterprises are increasingly looking for ways to streamline their support processes and reduce fixed costs while maintaining high service levels and operational efficiency.

Improved Security: A centralized remote access solution can enhance security protocols, addressing concerns about fragmented practices that may lead to vulnerabilities.

Support for Varied IT Environments: With a mix of devices and use cases, businesses need remote access solutions that can accommodate various connectivity options, ensuring reliable access across different setups, whether online or offline.

Consolidation of Software: Fragmented purchasing decisions often lead to multiple similar tools being used across departments. Centralizing software not only enhances security and compliance but also improves negotiating power, driving better value from vendors.

Increased Efficiency Ultimately, remote access solutions should empower IT teams to support their organizations more effectively, minimise downtimes, and enhance productivity for remote-based teams.

CRITICAL FACTORS TO CONSIDER WHEN CHOOSING REMOTE ACCESS SOFTWARE

When selecting remote access software, several critical factors need to be evaluated to ensure that the solution not only meets current enterprise requirements but is also adaptable for future needs.

Scalability

The software must support a large number of users and devices across multiple locations without compromising performance. Look for solutions that offer ease of deployment, such as methods for deploying through Group Policy Objects (GPO). Additionally, consider how the ongoing management of users and devices will be handled, and ensure there are capabilities for tracking usage for auditing purposes.

Security and Compliance

Robust security measures are paramount in safeguarding sensitive data. Evaluate encryption

standards, access controls, and the software's compliance with industry regulations, such as the GDPR and HIPAA. For added protection, Multi-Factor Authentication (MFA) methods should be implemented. It's also vital to understand if account credentials allow for connection authentication and whether that level of security is sufficient for your business needs; for instance, RealVNC does not allow device access via account credentials, unlike TeamViewer.

Performance

Performance metrics, including speed, latency, and reliability in various network conditions, are essential for user satisfaction, especially when operating within a larger business environment. Ensure that the chosen solution can deliver consistent performance even under less-than-ideal network circumstances to maintain productivity.

Compatibility

Compatibility with existing systems, applications, and devices is crucial. Assess if the software supports all required operating systems and whether it allows data utilization across different platforms. This consideration will help streamline operations and reduce potential integration issues.

Support and Training

Consider the level of enterprise-level support offered by the software provider. Availability of training resources and responsive customer service will determine how effectively IT teams can implement and manage the software. Usability is also a significant factor; IT teams should avoid tools that necessitate extensive upskilling or handholding for employees, as this can lead to frustration and decreased productivity.

Evaluating these critical factors will empower enterprises to select an effective remote access solution that aligns with their operational

requirements while enhancing security, compliance, and overall efficiency.

Deployment is another crucial area to explore. When selecting a remote access solution, consider the following types of deployment:

- Cloud v Direct Connectivity
- Installed v On-Demand Access
- On-Premise Solution

“...Manufacturing organizations use an average of just under three different solutions.”



A GUIDE FOR ENTERPRISES

(A) CLOUD VS. DIRECT CONNECTIVITY:

When selecting remote access solutions for large businesses, it's crucial to understand the differences between cloud and direct connectivity. Each method offers unique advantages and potential drawbacks, which can impact the efficiency and security of remote operations.

Direct Connections for Enterprises

Direct connections allow you to establish (and maintain) a connection exclusively between devices, with neither of the endpoints or data communicating with third-party servers. This method benefits enterprises requiring tighter control over their data and network parameters.

...Such control allows for configurations tailored to specific organizational needs...

such as ensuring sensitive information transfers remain within a private network. However, implementing direct connections can be intricate,

necessitating knowledge of the target computer's IP address or hostname and often requiring complex port forwarding and firewall adjustments. This setup can be a barrier, especially in environments with restrictive network infrastructures, like hotels or public Wi-Fi, where modifications cannot be made by an IT team, potentially hindering effective remote support.

Cloud Connections for Enhanced Scalability

Conversely, cloud connections present a highly scalable solution that simplifies remote access for large organizations. By leveraging the cloud, enterprises can establish seamless connections without adjusting existing firewalls or routers, making it ideal for employees working remotely or traveling. Regardless of the location, as long as both endpoints are connected to the Internet, cloud services facilitate quick, efficient connections. Notably, these connections often transition to a peer-to-peer model, optimizing latency and enhancing the user experience. Additionally, security is fortified as cloud services typically incorporate advanced protections against cyber threats, such as man-in-the-middle attacks.

Making the Right Choice for Your Enterprise

The ideal choice between cloud and direct connectivity will largely depend on your enterprise's specific operational requirements and potential security considerations. Large businesses

frequently operate in dynamic environments, with employees working from various locations, making cloud solutions appealing due to their flexibility and ease of use. However, the direct connection approach may provide the necessary control for organizations dealing with sensitive data. As a strategic recommendation, enterprises should consider adopting remote access software accommodating both connection methods. This dual capability ensures robust, secure, and adaptable remote access, preparing organizations for various connectivity scenarios while maintaining operational efficiency.

A GUIDE FOR ENTERPRISES

(B) INSTALLED VS. ON-DEMAND ACCESS:

When considering remote access solutions, enterprises must decide between installed and on-demand access, each catering to distinct use cases and operational needs.

Installed Access

For organizations able to pre-install remote access software, installed access significantly broadens the range of possible applications. This method allows for repeated connections to remote computers,

whether they are your own devices or those of employees and colleagues, facilitating both attended and unattended sessions. The ability for multiple users to connect concurrently enhances collaboration and eases information sharing, making it an ideal choice for training sessions or support demonstrations. However, this approach requires careful planning and appropriate permissions to ensure software deployment across all necessary devices, which can be a logistical challenge in large enterprises.

On-Demand Access

On the other hand, on-demand access is tailored for scenarios where installing software in advance is not feasible.

This model is beneficial in environments like Bring Your Own Device (BYOD) policies...

or when providing customer support. With on-demand access, the software is provisioned 'just in time'—installed when support is needed and removed afterward to leave no trace on the remote machine. While this approach can streamline support processes and enhance user privacy, it typically lacks features like unattended access, making it less suitable for ongoing administrative tasks or scenarios requiring direct connectivity.

Strategic Consideration

Enterprises should evaluate their operational contexts when choosing between installed and on-demand access, considering security, user control, and scalability. Adopting a versatile remote access solution, that supports both models, for organizations with diverse needs can provide a robust and secure framework.

This dual capability prepares businesses for various connectivity scenarios and ensures efficient resource management, ultimately enhancing the effectiveness of remote operations across the organization.

A GUIDE FOR ENTERPRISES (C) ON-PREMISE SOLUTIONS

On-premise remote access solutions provide enterprises with robust control over their data and infrastructure, making them a compelling choice for organizations prioritizing security and compliance. In general, on-premise deployments will make exclusive use of direct connections, whereby neither endpoints nor connection data communicate with third-party servers or external

networks; everything stays within the organization's networks and environment. By deploying software within their premises, businesses can tailor the system to their unique operational needs while adhering to regulatory standards.

Enhanced Security and Compliance

One of the primary advantages of on-premise solutions is their heightened security. By keeping sensitive data within the organization, businesses can significantly reduce the risk of external cyber threats commonly associated with cloud-based platforms. This aspect is especially critical for industries such as finance or healthcare, which require stringent compliance with data protection regulations. With on-premise solutions, businesses can implement comprehensive security measures—including access control, encryption, and regular audits—ensuring that sensitive information remains protected.

Customization and Integration

On-premise solutions allow for extensive customization, enabling enterprises to configure the software to align with their specific workflows and requirements. This flexibility can enhance operational efficiency, as organizations can adapt features and functionalities that best serve their teams.

Furthermore, on-premise systems can be designed to integrate seamlessly with existing IT infrastructure, fostering collaboration among various applications and tools that the organization relies on. This ultimately streamlines processes and improves productivity.

Resource Considerations

While the advantages of on-premise remote access solutions are considerable, enterprises should weigh the operational implications. Maintaining such a system often necessitates a dedicated in-house IT team with expertise to set up, manage, and continuously maintain the infrastructure. This requirement may pose resource challenges, particularly for smaller teams or organizations with limited IT budgets. To mitigate potential downsides, companies should assess their long-term commitment to operational support and consider the scalability of their on-premise solution to accommodate future growth.

Conclusion

In conclusion, on-premise remote access solutions deliver a powerful alternative for enterprises seeking secure, compliant, and customizable IT environments. By thoroughly evaluating their operational needs and resource capabilities, organizations can make informed decisions that ensure effective and efficient remote access while safeguarding critical data. As the remote work landscape continues to evolve, on-premise solutions stand out as a strategic option for businesses aiming to maintain control and security in their remote access initiatives.



COMPARING REMOTE ACCESS SOLUTIONS FOR ENTERPRISES

Using a comparison framework helps when assessing different remote access solutions. The framework below provides clarity and direction throughout the evaluation process. The following checklist categorizes features based on the critical factors outlined previously, allowing you to make informed decisions tailored to your organizational needs.

Quick Product Feature Comparison

Quick Comparison (Security)

	RealVNC® Connect	TeamViewer	AnyDesk	Splashtop
Default 2FA account verification	✓	✓	✗	✓
Decentralized device IDs	✓	✗	✗	✓
Default device authentication	✓	✗	✗	✓
2FA for connections	✓	✓	✓	✓
MFA (2+ methods) for connections	✓	✗	✗	✗
Granular user permissions	✓	✓	✓	✓
Activity logs	✓	✓	✗	✓
Single Sign-On	✓	✓	✓	✓
ISO 27001 Certified	✓	✓	✗	✓
HIPAA Compliant	✓	✓	✗	✓

Quick Comparison (Scalability)

Deploy via GPO	✓	✓	✓	✓
Management via API	✓	✓	✓	✓
Unlimited concurrent connections	✓	✗	✗	✓
SSO integration	✓	✓	✓	✓
3rd party integrations	✗	✓	✗	✓

Quick Comparison (Connectivity)

	RealVNC® Connect	TeamViewer	AnyDesk	Splashtop
Cloud-based connections	✓	✓	✓	✓
Direct (IP) connections over LAN	✓	✓	✓	✓
Attended remote access	✓	✓	✓	✓
Unattended remote access	✓	✓	✓	✓
On-demand remote support	✓	✓	✓	✓
On-premise deployment (inc. offline)	✓	✗	—	—

Quick Comparison (Interoperability)

Supported desktop platforms you can connect to remotely	Windows, macOS, Linux, PiOS	Windows, macOS, Linux, PiOS	Windows, macOS, Linux, PiOS, ChromeOS	Windows, macOS, Linux, PiOS
Supported desktop platforms you can connect from	Windows, macOS, Linux, PiOS	Windows, macOS, Linux	Windows, macOS, Linux, PiOS	Windows, macOS, Linux
iOS & Android	✓	✓	✓	✓
On-demand remote support	✓	✓	✓	✓

Evaluation Framework

Scalability

User Capacity:	⇒ How many users can be supported simultaneously without degradation in performance?
Deployment Methods:	⇒ Is the software easy to deploy across multiple locations, mainly through GPO?
Ongoing Management	⇒ Does the solution provide tools for streamlined management of users and devices?
Usage Tracking	⇒ Are there built-in capabilities for tracking usage to assist with auditing?

Security and Compliance

Speed:	⇒ How quickly does the software establish connections and transfer data?
Latency:	⇒ What is the expected latency in various network conditions?
Reliability:	⇒ Is the software's performance consistent during high traffic or poor network conditions?

Support and Training

Enterprise- Level Support:	⇒ What level of technical support is offered post-deployment?
Training Resources:	⇒ Are comprehensive training materials or sessions available for staff?
Usability:	⇒ How intuitive is the software for end-users? Does it require extensive training or support?

Security and Compliance

Encryption Standards:	⇒ What level of encryption is employed to protect data?
Access Controls:	⇒ How are user permissions managed? Are there customizable roles?
Regulatory Compliance:	⇒ Does the solution comply with necessary regulations, such as GDPR and HIPAA?
Multi-Factor Authentication:	⇒ Are MFA methods available to enhance security?
Connection Authentication:	⇒ How does the software handle connection authentication? Does it allow for device access via account credentials?

Compatibility

Operating Systems:	⇒ Can the software support all required operating systems within the enterprise?
Integration Capabilities:	⇒ How easily can it integrate with existing systems and applications?
Data Utilization:	⇒ Does the solution allow for data to be shared and utilized across different platforms seamlessly?

IMPLEMENTATION AND BEST PRACTICES

Implementing remote access software in a large enterprise environment requires meticulous planning and execution. Here are key steps and best practices to ensure a seamless transition while optimizing performance, maintaining security, and fostering user adoption.

Steps for Smooth Implementation

• Budget and Resources:

Establish a clear budget for software licensing, necessary hardware, and ongoing support costs. Ensure that resources are allocated for both financial and human capital.

• Stakeholder Buy-in:

Engage relevant stakeholders early in the process. This includes IT staff, management, and end-users, whose feedback and support are crucial for successful implementation.

• Project Management:

Develop a comprehensive project management plan with defined deliverables and timelines. Assign a dedicated project manager to oversee the implementation and ensure accountability throughout the stages.

• Internal Communication:

Maintain regular communication channels to inform all team members about progress, changes, and expectations. Transparency helps to alleviate concerns and prepare users for the transition.

• Training Programs:

Implement employee training sessions to facilitate a smooth onboarding experience. Provide comprehensive resources that cover software features, security protocols, and troubleshooting tips.

Best Practices for Optimising Performance and Maintaining Security

• Frequent Monitoring:

Regularly assess the remote access solution's performance to identify bottlenecks or vulnerabilities. Use analytics tools to monitor user activity and software performance metrics.

• Security Protocols:

Adhere to best security practices such as enforcing strong password policies, using MFA, regularly updating software, and conducting security audits. Ensure all users understand their responsibilities in maintaining security.

• User Adoption Strategies:

Encourage user feedback and address challenges promptly to foster a positive user experience. Highlight the benefits and efficiencies of the new solution, which can help drive adoption.

By following these implementation steps and best practices, enterprises can maximize the benefits of their remote access software, ensuring it aligns with their operational goals and enhances overall productivity.

GET THE ULTIMATE BUYER'S GUIDE TO REMOTE ACCESS TOOLKIT

Your All-in-One Guide to Purchasing and
Implementing Remote Access Solutions within
SMEs, Large and Enterprise Organizations



Toolkit Features:

- Budget and Financial Planning Documents
- Vendor Comparison Matrix and Selection Checklists
- Business Case Template for Switching Remote Access Provider
- Vendor Negotiation Strategy Document
- Implementation Roadmap Builder
- Technical Integration Guides and Change Management Plans



CONSIDERING REMOTE ACCESS SOFTWARE? TRY REALVNC® CONNECT

RealVNC Connect Enterprise lets your IT team
customize, deploy, and manage secure remote
access across your entire company with complete
confidence and control.

- Peace of mind security - 256-bit AES encryption, granular access controls, Multifactor Authentication (MFA)
- Scale with our Centralized Management Console
- Cross-Platform Support – Windows, macOS, Linux, iOS and Android
- High-Performance Connections – high quality screensharing, file transfer and remote printing
- APIs for custom integrations and automated device and user management
- White labelling options for On-Demand Assist
- Account SSO simplifies and secures login across your organization
- Priority support and a dedicated account manager
- Ensure compliance with audit and reporting tools
- Cost efficiency with flexible licensing
- Easy collaboration with multiple user control and session recording





BUYERS GUIDE

RealVNC®'s remote access and management software is used by hundreds of millions of people worldwide in every sector of industry, government and education. Our software helps organizations cut costs and improve the quality of supporting remote computers and applications. RealVNC is the original developer of VNC remote access software and supports an unrivalled mix of desktop and mobile platforms. Using our software SDKs, third-party technology companies also embed remote access technology direct into their products through OEM agreements.

Copyright © RealVNC® Limited 2024. RealVNC® and VNC® are trademarks of RealVNC® Limited and are protected by trademark registrations and/or pending trademark applications in the European Union, United States of America and other jurisdictions. Other trademarks are the property of their respective owners.

Protected by UK patents 2481870, 2491657; US patents 8760366, 9137657; EU patent 2652951